Claims:

1. A system comprising:

a participant subsystem that is authorized to anonymously participate in a plurality of sessions using secret information provided by a manager subsystem; and

a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session,

wherein

the participant subsystem comprises:

an anonymous signing section for authorizing individual data using the secret information depending on session-related information to produce anonymous participation data with anonymous signature, and

the reception subsystem comprises:

an anonymous signature determining section for determining whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem; and

a sender match determining section for determining whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

2. The system according to claim 1, wherein the anonymous signature includes data that is generated by a predetermined expression using the session-related information and the secret information, wherein the sender match determining section checks the data included in the anonymous signature of received anonymous participation data.

3. The system according to claim 2, wherein the predetermined expression is represented by raising a session-dependent base to a power that is dependent on the secret information.

4. The system according to claim 1, wherein the anonymous signing section authorizes the individual data based on a group signature scheme.

5. The system according to claim 1, wherein the anonymous signing section authorizes the individual data based on an escrowed identity scheme.

6. The system according to claim 1, wherein the anonymous signing section comprises:

a generator creating section for creating a session-dependent generator depending on the session-related information;

a group signing section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information; and

a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session-related information.

7. The system according to claim 6, wherein the secret information is represented by (x, y, v) that satisfies: $v = (y + \delta)^{1/e} \bmod n$, where $y = a^x \bmod n$, n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1,

the generator creating section creates a session-dependent generator g_A corresponding to a session A and a generator g_m is generated based on the individual data m and/or the session A.

the group signing section sets $z = g_A^{\gamma}$ and generates a first proof statement

$$V_1 = \mathrm{SKLOGLOG}(z, g_A, a)[\alpha : z = g_A^{(a^{\alpha})}] \quad (1)$$

proving the knowledge of α satisfying $z = g_A^{(\alpha^a)}$, and a second proof statement

V_2 = SKROOTLOG($z*g_A^b, g_A, e$)[β: $z*g_A^b = g_A^{(\beta^e)}$](1)

proving the knowledge of β satisfying $z*g_A^b = g_A^{(\beta^e)}$,

the linkage data generating section sets $z_1 = g_m^\gamma$, and generates a third proof statement

V_3 = SKREP(z_1/z, g_m/g_A)[γ: $z_1/z = (g_m/g_A)^\gamma$](1)

proving the knowledge of z_1 and z have the same power to the bases g_m and g_A, respectively,

wherein the anonymous participation data is defined as (A, m, z, z_1, V_1, V_2, V_3).

8. The system according to claim 7, wherein

the anonymous signature determining section checks V_1, V_2, and V_3 of the anonymous participation data to determine whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

the sender match determining section checks z of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

9. The system according to claim 1, wherein the anonymous signing section comprises:

a generator creating section for creating a generator depending on the session-related information;

a group signing section for signing the individual data using the generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information.

10. The system according to claim 9, wherein the secret information is represented by (x, y, v) that satisfies: $v = (y + \delta)^{1/e} \bmod n$, where $y = a^x \bmod n$, the individual data is denoted by m, n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1,

the generator creating section creates a session-dependent generator g_A corresponding to a session A,

the group signing section sets $z = g_A^{\,y}$ and generates a first proof statement

$$V_1 = \mathrm{SKLOGLOG}(z, g_A, a)[\alpha : z = g_A(a^{\alpha})](\mathrm{m})$$

proving the knowledge of α satisfying $z = g_A(a^{\alpha})$, and a second proof statement

$$V_2 = \mathrm{SKROOTLOG}(z * g_A^{\delta}, g_A, e)[\beta : z * g_A^{\delta} = g_A(\beta^{e})](\mathrm{m})$$

proving the knowledge of β satisfying $z * g_A^{\delta} = g_A(\beta^{e})$,

wherein the anonymous participation data 13 is designated as (A, m, z, V_1, V_2).

11. The system according to claim 10, wherein

the anonymous signature determining section checks V_1, and V_2 of the anonymous participation data to determine whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

the sender match determining section checks z of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

12. The system according to claim 1, wherein the anonymous signing section comprises:

a generator creating section for creating a session-dependent generator depending on the session-related information;

an escrow identifying section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information; and

a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session-related information.

13. The system according to claim 12, wherein the secret information is represented by (a, b) that satisfies $b = (a^e - \delta)^{1/e} \bmod n$, where n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1,

the generator creating section creates a session-dependent generator g_A corresponding to a session A and a generator g_m is generated based on the individual data m and/or the session A,

the escrow identifying section sets $z_a = g_A^{(a^e)}$ and generates a first proof statement

$$V_1 = \mathrm{SKROOTLOG}(z_a, g_A, e)[\alpha: z_a = g_A^{(\alpha^e)}](1)$$

proving the knowledge of α satisfying $z_a = g_A^{(\alpha^e)}$, and sets $z_b = g_A^{(b^e)}$ and generates a second proof statement

$$V_2 = \mathrm{SKROOTLOG}(z_b, g_A, e)[\beta: z_b = g_A^{(\beta^e)}](1)$$

proving the knowledge of β satisfying $z_b = g_A^{(b^d)}$, and

the linkage data generating section sets $z_c = g_m^{(a^e)}$ and generates a third proof statement

$$V_3 = \mathrm{SKREP}(z_c/z_a, g_m/g_A)[\gamma: z_c/z_a = (g_m/g_A)^\gamma](1)$$

proving the knowledge of z_a and z_c having the same power to the bases g_A and g_m, respectively,

wherein the anonymous participation data is defined as $(A, m, z_a, z_b, z_c, V_1, V_2, V_3)$.

14. The system according to claim 13, wherein

the anonymous signature determining section determines whether $z_a/z_b = g_A^{\delta}$ is satisfied and checks V_1, V_2, and V_3 of the anonymous participation data to determine whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

the sender match determining section checks one of z_a and z_b of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

15. The system according to claim 1, wherein the anonymous signing section comprises:

a generator creating section for creating a session-dependent generator depending on the session-related information; and

an escrow identifying section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data,

wherein the anonymous participation data includes data

obtained by raising the session-dependent generator to a power determined by the secret information.

16. The system according to claim 15, wherein the secret information is represented by (a, b) that satisfies $b = (a^e - \delta)^{1/e} \bmod n$, where n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1,

the generator creating section creates a session-dependent generator g_A corresponding to a session A,

the escrow identifying section sets $z_a = g_A{}^{(a^e)}$ and generates a first proof statement

$V_1 = \mathrm{SKROOTLOG}(z_a, g_A, e)[\alpha: z_a = g_A{}^{(\alpha^e)}](m)$

proving the knowledge of α satisfying $z_a = g_A{}^{(a^e)}$, and sets $z_b = g_A{}^{(b^e)}$ and generates a second proof statement

$V_2 = \mathrm{SKROOTLOG}(z_b, g_A, e)[\beta: z_b = g_A{}^{(\beta^e)}](m)$

proving the knowledge of β satisfying $z_b = g_A{}^{(b^e)}$,

wherein the anonymous participation data is defined as $(A, m, z_a, z_b, V_1, V_2)$.

17. The system according to claim 16, wherein

the anonymous signature determining section determines whether $z_a/z_b = g_A{}^{\delta}$ is satisfied and checks V_1 and V_2 of the anonymous participation data to determine whether

received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

the sender match determining section checks one of z_a and z_b of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

18. An anonymous participation authority management method for a system comprising:

a participant subsystem that is authorized to anonymously participate in a plurality of sessions using secret information; and

a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session,

the method comprising the steps of:

at the participant subsystem,

a) authorizing individual data using the secret information depending on session-related information to produce anonymous participation data with anonymous signature;

at the reception subsystem,

b) determining whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem; and

c) determining whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

19. The method according to claim 18, wherein the anonymous signature includes data that is generated by a predetermined expression using the session-related information and the secret information, wherein the step (c) is performed by checking the data included in the anonymous signature of received anonymous participation data.

20. The method according to claim 19, wherein the predetermined expression is represented by raising a session-dependent base to a power that is dependent on the secret information.

21. The method according to claim 18, wherein the step (a) comprises the steps of:

creating a session-dependent generator depending on the session-related information;

signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information; and

generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session-related information.

22. The method according to claim 18, wherein the step (a) comprises the steps of:

creating a session-dependent generator depending on the session-related information; and

signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information.